PCT/IL04/000903

iL04/00903

מדינת ישראל
STATE OF ISRAEL

Ministry of Justice
Patent Office

משרד המשפטים
לשכת הפטנטים

This is to certify that annexed hereto is a true copy of the documents as originally deposited with the patent application particulars of which are specified on the first page of the annex.

זאת לתעודה כי רצופים בזה העתקים נכונים של המסמכים שהופקדו לכתחילה עם הבקשה לפטנט לפי הפרטים הרשומים בעמוד הראשון של הנספח.

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

LIBRARY
ISRAEL
PATENT OFFICE

This 14-10-2004 היום

Commissioner of Patents
ממונה על רשם הפטנטים

נתאשר
Certified

PCT REQUEST

Original (for **SUBMISSION**)

0	**For receiving Office use only**	
0-1	International Application No.	**PCT/IL** 2004/000806
0-2	International Filing Date	07 SEP 2004 (07.09.2004)
0-3	Name of receiving Office and "PCT International Application"	ISRAEL PATENT OFFICE PCT International Application
0-4	**Form PCT/RO/101 PCT Request**	
0-4-1	Prepared Using	PCT-SAFE [EASY mode] Version 3.50 (Build 0002.162)
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	Israel Patent Office (RO/IL)
0-7	**Applicant's or agent's file reference**	279/04169
I	**Title of Invention**	SECURE MULTICAST TRANSMISSION
II	**Applicant**	
II-1	This person is	applicant only
II-2	Applicant for	all designated States except US
II-4	Name	BAMBOO MEDIACASTING LTD.
II-5	Address	P.O. BOX 5035 44150 KFAR SABA Israel
II-6	State of nationality	IL
II-7	State of residence	IL
II-8	Telephone No.	+972 9 746 4676
II-9	Facsimile No.	+972 9 746 4674
III-1	**Applicant and/or inventor**	
III-1-1	This person is	applicant and inventor
III-1-2	Applicant for	US only
III-1-4	Name (LAST, First)	ENTIN, Leonid
III-1-5	Address	10 ADMONIT STREET 71700 MODIIN Israel
III-1-6	State of nationality	IL
III-1-7	State of residence	IL

PCT REQUEST

Original (for SUBMISSION)

III-2	**Applicant and/or inventor**	
III-2-1	This person is	applicant and inventor
III-2-2	Applicant for	US only
III-2-4	Name (LAST, First)	AMRAM, Noam
III-2-5	Address	12 TCHARNIHOVSKI STREET 58382 HOLON Israel
III-2-6	State of nationality	IL
III-2-7	State of residence	IL
III-3	**Applicant and/or inventor**	
III-3-1	This person is	applicant and inventor
III-3-2	Applicant for	US only
III-3-4	Name (LAST, First)	FUCHS, Meir
III-3-5	Address	18/4 NAHAL HAYARKON STREET 71700 MODYIN Israel
III-3-6	State of nationality	IL
III-3-7	State of residence	IL
IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name (LAST, First)	FENSTER, Paul
IV-1-2	Address	FENSTER & COMPANY, INTELLECTUAL PROPERTY 2002 LTD. P. O. BOX 10256 49002 PETACH TIKVA Israel
IV-1-3	Telephone No.	+972 (3) 921-5380
IV-1-4	Facsimile No.	+972 (3) 921-5383
IV-1-5	e-mail	fensterco@fenster.co.il
IV-2	**Additional agent(s)**	additional agent(s) with same address as first named agent
IV-2-1	Name(s)	FENSTER,Maier; ENTIS,Allan; SCHATZ,Yaakov

279/04169

PCT REQUEST

Original (for **SUBMISSION**)

V	**DESIGNATIONS**		
V-1	**The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.**		
VI-1	**Priority claim of earlier national application**		
VI-1-1	Filing date	11 September 2003 (11.09.2003)	
VI-1-2	Number	157886	
VI-1-3	Country	IL	
VI-2	**Priority document request** The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as Ite m(s):	VI-1	
VII-1	**International Searching Authority Chosen**	United States Patent and Trademark Office (USPTO) (ISA/US)	
VIII	**Declarations**	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	-	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	-	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	-	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	-	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	-	
IX	**Check list**	number of sheets	electronic file(s) attached
IX-1	Request (including declaration sheets)	4	✓
IX-2	Description	17	-
IX-3	Claims	7	-
IX-4	Abstract	1	✓
IX-5	Drawings	2	-
IX-7	TOTAL	31	

279/04169

PCT REQUEST

Original (for SUBMISSION)

	Accompanying Items	paper document(s) attached	electronic file(s) attached
IX-8	Fee calculation sheet	✓	-
IX-11	Copy of general power of attorney	✓	-
IX-17	PCT-SAFE physical media	-	✓
IX-19	**Figure of the drawings which should accompany the abstract**	1	
IX-20	**Language of filing of the international application**	English	
X-1	**Signature of applicant, agent or common representative**	Paul Fenster	
X-1-1	Name (LAST, First)	FENSTER, Paul	
X-1-2	Name of signatory		
X-1-3	Capacity		

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	07 SEP 2004 (07.09.2004)
10-2	**Drawings:**	
10-2-1	Received	↘
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/US
10-6	**Transmittal of search copy delayed until search fee is paid**	↘

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	

279/04169

PCT REQUEST (ANNEX - FEE CALCULATION SHEET)

Original (for **SUBMISSION**)

(This sheet is not part of and does not count as a sheet of the International application)

0	**For receiving Office use only**	
0-1	International Application No.	PCT/IL2004/000806
0-2	Date stamp of the receiving Office	07 SEP 2004 (07.09.2004)

0-4	**Form PCT/RO/101 (Annex) PCT Fee Calculation Sheet**				
0-4-1	Prepared Using	PCT-SAFE [EASY mode] Version 3.50 (Build 0002.162)			
0-9	**Applicant's or agent's file reference**	279/04169			
2	**Applicant**	BAMBOO MEDIACASTING LTD.			
12	**Calculation of prescribed fees**		fee amount/mulipiler	Total amounts (ILS)	Total amounts (USD)
12-1	Transmittal fee	T	⇨	476	
12-2-1	Search fee	S	⇨		1000
12-2-2	International search to be carried out by		US		
12-3	International filing fee (first 30 sheets)	I1	1134 USD		
12-4	Remaining sheets		1		
12-5	Additional amount	(X)	12 USD		
12-6	Total additional amount	I2	12 USD		
12-7	I1 + I2 =	I	1146 USD		
12-12	EASY Filing reduction	R	USD-81		
12-13	Total International filing fee (I-R)	I	⇨		1065
12-14	Fee for priority document				
	Number of priority documents requested		1		
12-15	Fee per document	(X)	0 ILS		
12-16	Total priority document fee:	P	⇨		
12-17	**TOTAL FEES PAYABLE (T+S+I+P)**		⇨	476	2065
12-19	**Mode of payment**		other Please bill us.		

PCT

Original (for SUBMISSION)

13-2-7	Validation messages Contents	Green? Reference number for attached copy of general power of attorney not indicated.

SECURE MULTICAST TRANSMISSION

FIELD OF THE INVENTION

The present invention relates generally to communication networks and particularly to methods of preventing unauthorized dissemination of multicast data.

BACKGROUND OF THE INVENTION

Cellular phones can be used for receiving video clips and other data, in addition to their use for point to point telephone communication. Multicasting the data to the cellular phones or to other mobile stations allows efficient use of the available bandwidth, such that large amounts of data can be provided to the cellular phones without requiring prohibitive amounts of bandwidth. In some cases, users are required to subscribe and pay for the multicast data if they desire to receive the data. In order to prevent other cellular phones that were not subscribed to the data from receiving the data without paying, the data is encrypted and only subscribers are provided with the decryption key. A problem arises, however, if one of the subscribers disseminates the key to other users, allowing the other users to decrypt the data without paying. It is noted that while a subscriber could forward the entire data to other users, this would be very costly in cellular networks, generally more than the cost of subscription.

US patent publication 2003/0046539 to Negawa, the disclosure of which is incorporated herein by reference, suggests periodically changing the key and providing the keys to the subscribers on encrypted private unicast channels. This solution, however, is not suitable for a sophisticated disseminating user who continuously provides the keys to other users immediately when the new keys are received.

US patent publication 2002/0039361, to Hawkes et al., the disclosure of which is incorporated herein by reference, suggests supplying each mobile station with a special processing and storage module which is adapted for storing keys and other secret information, without the information being available to the user for dissemination. Such solution requires that all users buy special hardware in order to receive the multicast data and therefore is unpractical.

US patent publication 2002/0138826 to Peterka, the disclosure of which is incorporated herein by reference, suggests transmitting the multicast data in a few copies with different keys. Each copy of the multicast data is provided with a different rate of changing decryption keys. A subscribing user pays for data for a predetermined amount of time and accordingly is provided with a key for a group having a key replacement timing fitting the time for which the

user paid. Thus, change of keys is not required when a user leaves the group. However, no method of discouraging sharing of the keys is described.

US patent publication 2002/0136407, to Denning et al., describes a method of encrypting data such that it can be decrypted only if it passed through a predetermined path, at a predetermined location or during a predetermined time range. The sender encrypts the data directed to each location with an encryption key related to the location of the receiver. This method is not suitable for multicast and is not suggested for multicast.

SUMMARY OF THE INVENTION

An aspect of some embodiments of the invention relates to a method of multicast delivery of a data file to receivers. The method includes encrypting the data file and providing one or more keys required for decrypting the file only after the data is provided to the receiver. Providing the keys only after transmission of the data allows having the receivers request for the keys, so that the requests serve as acknowledgement of receiving the data file.

An aspect of some embodiments of the invention relates to a method of multicasting a data block to a plurality of receivers. The block is represented by a plurality of data segments which include redundancy, such that the block can be determined in its entirety even if fewer than all the segments are received. It is noted that some of the data segments may be identical. The segments are divided into groups which are encrypted using different keys. In order to decrypt the block, the receiver optionally requests, from a control unit, the keys it needs for the segments it received. The segments are transmitted in a manner such that different receivers receive segments requiring different keys and therefore require different sets of keys to decrypt the segments and reconstruct the block. A receiver requesting the keys cannot generally distribute the keys to other receivers on a large scale, as the keys will not be usable, based on statistical analysis, by more than a few other receivers.

In some embodiments of the invention, the keys are transmitted on a high loss channel, such that different receivers receive different segments due to the losses of the channel. Alternatively or additionally, different portions of the segments are transmitted on different channels (e.g., different time slots, frequencies, codes), and different receivers tune on to different channels. Optionally, receivers may tune on to a single channel during the entire transmission or may switch between channels during the transmission. In some embodiments of the invention, each receiver is preconfigured with one or more channels to which it listens.

Further alternatively or additionally, different segments are transmitted in different localities, from different multicasting points, for example from different base stations of a

cellular network. A receiver may optionally regenerate the block using a valid set of segments collected from a plurality of different multicasting points, and is not limited to segments from a single multicasting point. Thus, a receiver moving during the transmission between different multicasting points can use the data received from different multicast points.

The data segments are optionally generated and encrypted at a single source point, and are transmitted from the source point to the multicasting points on respective unicast channels, optionally passing on cables connecting the source point to the multicast points. As the cost of wireless bandwidth is much higher than the cost of terrestrial bandwidth, the additional cost of distributing different segments or different keys to the multicast points by land lines is relatively small.

Alternatively, the segments are not encrypted (or are encrypted using a different method) on their way to the multicasting points, and the encryption is performed by the multicasting points. In this alternative, the segments may be multicast to the multicasting points, over a cabled network or wirelessly using encryption or frequencies not available to the end user, thus reducing the amount of bandwidth used for distributing the data to the multicasting points. Further alternatively, the data is broken up into segments or is generated at the multicasting points or on the way to the multicasting points.

In some embodiments of the invention, the segments representing the block include FEC encrypted segments, such that a receiver collecting a predetermined number (m) of segments out of the (n) transmitted segments can reconstruct the block. Optionally, sub-groups of the FEC segments, including one or more segments, are encrypted with different keys. If many of the receivers receive the block on a high loss rate channel, such that they receive only m or a few more than m segments, the receivers will generally require different sets of keys for decryption.

Optionally, the keys are changed with time, for example after transmission of every few segments. Alternatively, the segments encrypted with same keys are interleaved between segments encrypted with other keys.

In some embodiments of the invention, the encryption segments are smaller than or equal the size of the FEC segments, such that they do not extend beyond the border between two FEC segments. Thus, an error in a transmitted encryption segment affects only a single FEC segment.

The methods for discouraging key sharing of the present invention may optionally be used with substantially any coding method, from very simple methods to very complex

methods. It is noted, however, that using the methods of the present invention serves in itself as a relatively high barrier to illegitimate decryption on a large scale and therefore, relatively simple coding methods, such as symmetric encryption may be used.

The methods of the present invention are generally applied to the data itself and not to keys which are used to encrypt the data. Therefore, a user who rightfully receives the keys to the data cannot easily transfer the decrypted data to a different user, as this would require transferring very large amounts of data.

An aspect of some embodiments of the present invention relates to transmitting same multicast data through a plurality of base stations with different encryption for each of the base stations. In some embodiments of the invention, a mobile station receiving a first portion of the data from a first base station and a second portion of the data from a second base station can reconstruct the data, although the first and second portions were encrypted with different encryption. The different encryption optionally includes use of a different key and/or a different encryption method. Using different encryption schemes for data transmitted by different base stations, limits the possibility of illegal disseminating decryption keys, as keys suitable for data of one base station are not suitable for other base stations.

There is therefore provided, in accordance with an embodiment of the invention, a method of multicasting data, comprising providing a data block for multicasting, generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block, encrypting at least a portion of the generated segments, so as to generate encrypted data units encrypted with a plurality of different keys or encryption methods and transmitting the encrypted data units over one or more multicast channels.

Optionally, generating the plurality of segments comprises generating forward error correction (FEC) segments, such that any group of a predetermined number of non-identical segments can be used to reconstruct the data block. Optionally, generating the plurality of segments comprises generating segments that include a portion of the data block.

Optionally, the plurality of segments include at least one set of duplicate segments.

Optionally, encrypting at least a portion of the segments comprises encrypting such that each data unit represents data from a single segment. Optionally, encrypting at least a portion of the segments comprises encrypting each segment into a single encrypted data unit. Alternatively or additionally, encrypting at least a portion of the segments comprises encrypting data of each segment into a plurality of encrypted data units. Optionally, encrypting

data of each segment into a plurality of encrypted data units comprises leaving a portion of each segment not encrypted. Optionally, the non-encrypted portions of the segments are used for transferring preview information. Optionally, the non-encrypted portions are located in different positions in different segments. Alternatively, the non-encrypted portions are located in same positions of substantially all the segments.

Optionally, encrypting at least a portion of at least some of the segments comprises encrypting using a symmetric coding scheme. Optionally, encrypting using a plurality of different keys or methods comprises encrypting using different keys and substantially same methods. Alternatively or additionally, encrypting using a plurality of different keys or methods comprises encrypting using different methods. Optionally, transmitting the encrypted data units comprises transmitting through a plurality of transmission points each of which transmits to different areas. Optionally, transmitting the encrypted data units comprises transmitting through a plurality of base stations. Optionally, each transmission point transmits sufficient data required for reconstruction of the data block.

Optionally, at least some of the transmission points transmit data units representing identical segments encrypted using different keys or methods. Optionally, the transmission points of at least one group of two or more transmission points transmit data units representing identical segments encrypted using same keys and methods. In some embodiments of the invention, the transmission points included in a group that transmit data units representing identical segments encrypted using same keys and methods vary dynamically over time.

Optionally, at least one of the transmission points transmits data units encrypted using a plurality of different keys or methods. Optionally, the encrypted data units are transmitted along with an identification of the respective key required to decrypt the data unit. Optionally, the identification of the key includes a portion which depends on the transmission point through which the data unit is transmitted. Optionally, the encrypted data units are transmitted along with an identification of the respective key required to decrypt the data unit. Optionally, the identification of the key is included in a field including redundancy, such that only some of the possible values of the field are valid identifications of keys. Optionally, encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels, less than a predetermined percentage of receivers of the data block will require, on the average, the same set of keys for decryption.

Optionally, encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels,

less than ten percent of the receivers of the data block will require on the average the same set of keys for decryption. Optionally, encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels, less than one percent of the receivers of the data block will require on the average the same set of keys for decryption. Optionally, the method includes receiving requests for keys required for decryption and keeping track of receivers that request a suspiciously large number of keys and/or request keys corresponding to non-existent identifications. Optionally, substantially all the encryption is performed at the same unit. Alternatively, the encryption of different segments is performed by different units.

There is further provided in accordance with an embodiment of the invention, a method of receiving multicast data over a transmission network, by a mobile station, comprising receiving one or more data units of a data block, from each of a plurality of multicast transmission points, the data units of each transmission point being encrypted using different respective one or more keys, decrypting the data units and reconstructing the data block from the decrypted data units, which were received from the plurality of multicast transmission points.

Optionally, the method includes determining from the received data units identification of the keys required in order to decrypt the data units and requesting the required keys from a key server. Optionally, the identifications of the keys depend, at least partially, on the multicast transmission point through which the data units are received, such that data units transmitted through different transmission points include different key identifications. Optionally, the multicast transmission points include base stations and/or wireless LAN access points.

There is further provided in accordance with an embodiment of the invention, a method of multicasting data, comprising providing a data block for multicasting, generating a plurality of different sets of encrypted segments requiring different sets of decryption keys, to represent the data block, and transmitting each of the different sets of encrypted segments from a different multicast transmission point.

Optionally, generating the plurality of different sets of encrypted segments comprises generating a single set of non-encrypted segments and generating the plurality of different sets of encrypted segments by encrypting the non-encrypted segments using a plurality of different encryption keys. Optionally, generating the plurality of different sets of encrypted segments comprises encrypting each of the plurality of different sets using groups of different keys. Optionally, the groups of different keys do not include any common keys. Optionally, the

transmission points comprise base stations of a cellular network. Optionally, generating the plurality of different sets of encrypted segments is performed in a single encryption unit. Optionally, at least part of the generating of the sets of encrypted segments is performed separately for each set in respective processors associated with the transmission points. Optionally, each of the encrypted segments includes a key identification field which identifies the key required to decrypt the segment.

Optionally, the method includes providing keys required for decrypting a plurality of sets of segments to a single receiver. Optionally, the method includes providing no more than 50% of the keys used for segments related to the data block to any single receiver.

There is further provided in accordance with an embodiment of the invention, a method of multicasting data, comprising providing a data block, generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block, encrypting a portion of each of the generated segments, so as to generate respective transmission segments including both encrypted and non-encrypted data and transmitting the transmission data units over a multicast channel.

There is further provided in accordance with an embodiment of the invention, a method of multicast transmission comprising providing a data block, encrypting the data block utilizing at least one given key, multicast transmitting the encrypted data block, requesting the at least one key by a receiver that receives the encrypted data block and unicast transmitting the at least one key to the receiver.

Optionally, encrypting the data block comprises generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block and encrypting at least some of the segments.

Optionally, encrypting at least some of the segments comprises encrypting one or more of the segments utilizing a first key and using at least one other key for at least one other segment. Optionally, requesting the at least one key comprises requesting based on an identification of the key included in the transmission. Optionally, the identification of the key is included in a field that can receive more values than valid identification values. Optionally, the method includes identifying receivers that request a suspiciously large number of keys or request non-existent keys. Optionally, requesting the at least one key is performed only after the receiver determined that a sufficient amount of data was received to allow reconstruction of the data block.

BRIEF DESCRIPTION OF FIGURES

Particular non-limiting embodiments of the invention will be described with reference to the following description of embodiments in conjunction with the figures. Identical structures, elements or parts which appear in more than one figure are preferably labeled with a same or similar number in all the figures in which they appear, in which:

Fig. 1 is a schematic illustration of a cellular network, useful in explaining an exemplary embodiment of the present invention; and

Fig. 2 is a flowchart of acts performed by a mobile station in receiving a file, in accordance with an exemplary embodiment of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS

Fig. 1 is a schematic illustration of a cellular network 100, in accordance with an exemplary embodiment of the present invention. Network 100 includes a plurality of base stations 50, which transmit signals to mobile stations 20 in their vicinity. In transmission of multicast data to mobile stations 20, a data source 30 generates files which are to be multicast to subscribing mobile units 20. Optionally, the generated files are broken into blocks of predetermined size, suitable for processing. The blocks are optionally passed to a forward error correction (FEC) unit 32, where a plurality of segments are prepared to represent the block. Optionally, N segments are prepared, such that any M (M<N) of the N segments can be used to reconstruct the block. The FEC segments may be generated using substantially any FEC method known in the art, including one-dimensional, two-dimensional, systematic and non-systematic methods. In an exemplary embodiment of the invention, a FEC method such as described in PCT patent application PCT/IL2004/000204, filed March 3, 2004 and/or in Israel patent application 157,885, titled "Iterative Forward Error Correction", filed September 11, 2003, the disclosures of which are incorporated herein by reference, is used. The FEC segments are optionally transferred to an encryption unit 34, which encrypts the FEC segments, forming respective encrypted segments.

The encrypted segments of each base station 50 are optionally transferred through a terrestrial network 40 of cellular network 100 to their intended base station, from which they are transmitted to mobile stations 20. Base stations 50 operate as multicast transmission points from which transmitted segments of the same data are all identical. The segments from data source 30 to base stations 50 may be different for different segments although they carry the same data. The segments are transmitted to mobile stations 20 using any multicast method known in the art, such as the method described in PCT publication WO03/019840 published

March 6, 2003, the disclosure of which is incorporated herein by reference. Optionally, each encrypted segment is transmitted as a respective RLC segment using methods known in the art.

Network 100 optionally includes a key server 36 which provides decryption keys to mobile stations 50. In some embodiments of the invention, users receiving the block (or the entire file), desiring to read the block, contact key server 36 and request the keys they need for the decryption. Alternatively or additionally, some of the keys are provided in multicast, and the users request only the keys that they need which were not multicast to them.

In some embodiments of the invention, for each base station 50, encryption unit 34 prepares differently encrypted segments, using keys which are different from those for the other base stations. Alternatively or additionally, some base stations use the same keys or use partially overlapping groups of keys, in order to limit the number of keys managed by encryption unit 34. Optionally, base stations separated by large distances use the same keys or a partial group of overlapping keys. Alternatively or additionally, base stations generally having small numbers of users use keys which are also used by other base stations. Further alternatively or additionally, all base stations 50 in a same region and/or controlled by a same controller, e.g., a same point-to-multipoint unit PTMU (introduced below) and/or base station controller (BSC), use the same keys.

Optionally, the size of a region of base stations that use the same keys is selected such that a moving mobile will not pass through more than a predetermined number (e.g., 10-20) regions having different keys, so as to limit the number of keys that moving receivers need to request. In some embodiments of the invention, when a region uses more than one key for a single file, the total number of keys that a moving receiver will need to request is limited to less than a predetermined number of keys (e.g., less than 20, 30 or 50). Optionally, the sizes of the regions that have the same keys depend on the expected movement speed of the receiver. For regions in which fast movement is allowed through a large number of cells (i.e., areas governed by respective base stations), the number of neighboring base stations sharing common keys is relatively large (e.g., greater than 10-20). Conversely, in regions in which movement is relatively slow and/or cells are relatively large, the number of cells sharing keys is relatively small (e.g., smaller than 10 or even 6).

Alternatively to sharing keys by neighboring cells, the cells that share keys are close cells that are separated by one or more intervening cells. Thus, a moving receiver does not need many keys, but neighboring receivers cannot necessarily use the same keys.

In some embodiments of the invention, base stations sharing keys share all their keys. Alternatively or additionally, some or all base stations that share keys share only some of their keys.

The base stations that share keys may be predetermined groups of base stations. Alternatively, in order to make unauthorized dissemination of keys more difficult, the grouping of the base station using same keys varies in real time. In some embodiments of the invention, the base station grouping varies every few hours or days. Alternatively, the base station groupings change every few moments and/or for every transmitted message or for every small number (e.g., up to 5-10) of messages. Further alternatively or additionally, the base station groupings may be changed within the transmission of a single message.

In some embodiments of the invention, the grouping of the base stations is changed randomly or in a pseudo random manner in order to prevent hackers from determining the grouping patterns. Alternatively or additionally, the grouping is adjusted according to the load on the network. Optionally, when the network is relatively loaded, fewer keys are used, for example having adjacent base stations use the same keys. This reduces the amount of bandwidth required for disseminating the keys and for providing the data to the base stations. When the network is relatively not loaded, more keys are used, to allow for better protection of the data. Alternatively or additionally, the local diversity of encryption keys is configurable by a network operator.

Each base station 50 optionally uses a plurality of different keys for the segments of a single block. The number of keys used in encrypting the data of a single block for a single base station 50 is optionally determined as a compromise between using a large number of keys required for key diversity which prevents illegitimate dissemination of keys and a small number of keys, which reduces the amount of bandwidth spent on dissemination of keys to users. In an exemplary embodiment of the invention, a different key is used for about every 10-20 segments. Optionally, segments that are encrypted with the same key include sequential portions of data from the block. This option reduces the number of keys a user requires on the average. Therefore, users requiring a large number of keys raise more suspicion that they disseminate keys to others. Alternatively, segments encrypted with the same key are taken from separated portions of the block such that the segments encrypted with a single key are interleaved between segments encrypted with other keys.

In some cases, some or all of the data segments of the block are transmitted a plurality of times in order to ensure proper reception, for example when mobile stations 20 may tune

onto the channel at different times. Optionally, each time the segments are transmitted they are encrypted with different keys.

In some embodiments of the invention, each transmitted segment includes a header which states the block and/or file to which it belongs, the position of the segment in an FEC array representing the block and an ID of the key required for decryption. The header is optionally not encrypted, so that the receiver can determine which segments are duplicates and can be discarded, whether a sufficient number of segments were received for reconstruction of the block and which keys are required for decrypting the segments. Alternatively or additionally, the segments are included in larger packets, for example IP packets, and the control information of the segment is included in a control section of the IP packet including the segment.

Optionally, the segment headers also include general information on the FEC method and/or encryption method. Alternatively or additionally, the general information is provided in the IP packets and/or at the beginning of the multicast. Further alternatively or additionally, the general information is provided on a separate channel, such as a broadcast channel describing the available multicast data and/or on a separate unicast channel used to provide the keys or for providing data at the beginning of the transmission.

Although data source 30, FEC unit 32, encryption unit 34 and key server 36 are shown as separate units, in some embodiments of the invention, one or more of these units are implemented by a single entity. For example, encryption unit 34 and key server 36 may be implemented on a single processor and/or may use a common key database. In some embodiments of the invention, data source 30 performs the task of FEC unit 32 and/or encryption unit 34 before forwarding the packets. In other embodiments of the invention, the encryption is performed at base stations 50 or at processors associated with each of the base stations. For example, the encryption may be performed at point to multi-point units (PTMUs) of the base stations, which PTMUs are described in the above mentioned PCT patent application PCT/IL2004/000204. Optionally, in these embodiments, the encryption ID is generated by each base station and/or PTMU from a static (i.e., changes infrequently if at all) code of the base station and a time dependent code which may be common to all base stations or is generated separately for each base station. Optionally, the static code is kept secret from the users, to make it harder on users to guess the encryption keys.

In some embodiments of the invention, two or more of the entities of network 100, for example encryption unit 34 and base stations 50, have the ability to encrypt the segments. The

unit that actually performs the encryption at any specific time optionally depends on the available processing resources on the units. For example, when the base stations are very loaded, the encryption is optionally performed by encryption unit 34.

Fig. 2 is a flowchart of acts performed by a mobile station in receiving a file, in accordance with an exemplary embodiment of the invention. The mobile station optionally tunes onto a multicast channel and receives (204) encrypted segments. The mobile station optionally verifies (206) that the packets were received without error. For example, the segments may include a CRC field, the value of which is used to check that the segment was received intact. The CRC check may be performed by an application layer performing the decryption and reconstruction or by a lower protocol layer. Segments that were received without error are optionally stored (208) in a memory of the mobile station. When a group of segments sufficient to allow reconstruction of a block is accumulated, the mobile station transmits (210) a message to key server 36, with IDs of the keys it requires in order to decrypt the segments it received. Optionally, the receiver knows that a sufficient number of packets were received when a predetermined number of packets sufficient for reconstruction were received. Alternatively, the receiver simulates the reconstruction, without actually performing the reconstruction which cannot be performed without the keys, in order to determine whether a sufficient number of packets were received. The simulations are optionally performed as described in the above mentioned Israel patent application 157,885.

Key server 36 transmits the keys generally on a unicast transmission, to the mobile station (211), which uses the keys to decrypt (212) the segments. Optionally, the keys are transmitted in a compressed format. The block is then reconstructed (214) from the decrypted segments according to the FEC method used.

In some embodiments of the invention, in storing (208) the received segments, the mobile unit discards segments carrying the same data (even if the segments were encrypted with a different encryption). Optionally, in any case a duplicate segment is received, the later received segment is discarded. Alternatively, if one of the duplicate segments can be opened with the same key as a different segment already received, the other copy of the duplicate segment is discarded. In some embodiments of the invention, a user not receiving a sufficient number of multicast segments required for reconstruction during the multicast transmission may request supplement of data on a unicast link, for example along with requesting the keys.

Key server 36 optionally keeps track of the mobile stations requesting keys, for billing purposes. In some embodiments of the invention, key server 36 keeps special track of mobile

stations that request particularly large sets of keys. Optionally, the content provider checks users that persistently, for many files, request large numbers of keys, to determine if they disseminate the keys to other users who are not being billed. In an exemplary embodiment of the invention, each file is transmitted 3-5 times with a 40-100% redundancy. In accordance with this exemplary embodiment, a request for about 25-30% of the keys is considered reasonable.

Alternatively or additionally to checking the number of keys requested, key server 36 checks whether there is a possibility that the requesting mobile station actually needs all the keys requested by the mobile station. For example, a mobile station requesting keys belonging to packets transmitted in locations separated by a distance which cannot be traveled during the entire transmission time of the file would be considered suspicious. In some embodiments of the invention, when a mobile station requests two keys which can only be used for the same segment (with different encryption) the reason is enquired.

Optionally, when a suspicious request for keys is received, an alarm message is sent to a controller of network 100. Alternatively or additionally, a periodic report on suspicious key requests is initiated. In some embodiments of the invention, location data on the mobile station initiating the suspicious request for keys is determined.

In some embodiments of the invention, the key IDs associated with the segments that are transmitted to key server 36 in requesting the keys, are not allocated in any consecutive order, but rather are selected randomly. This makes requesting keys for segments that the user did not receive, in order to disseminate the keys to other users who do not pay for the keys, harder. Optionally, the key IDs have a length which is sufficient to allow use of only some of the possible values in the keys, so as to make it more difficult for users to guess key IDs. Optionally, a manager of the network follows up on users that request non-existing keys. The length of the key ID field is optionally selected as a compromise between a long length which reduces the chances of illegal key dissemination and a short length which reduces the bandwidth required for key IDs. In an exemplary embodiment of the invention, the segment headers add an overhead of about 1-2%.

Alternatively to a single number serving as the key ID, the key ID may be formed of a plurality of fields, such as a first field identifying the base station 50 and a second field identifying the specific key used for the specific segment.

In some embodiments of the invention, different key IDs are used to represent the same key. This gives the advantage of using less bandwidth for providing the keys, while not

allowing the subscribers to know before asking for the keys that the keys are the same. For example, different cells may use different key IDs for same keys used in common by the cells.

Optionally, mobile stations do not request (210) any keys unless they received sufficient data to allow reconstruction of the block. Thus, the mobile station is not billed for the block or for a file unless the block was received in a manner which allows reconstruction. This prevents billing mobile stations for data they could not reconstruct, for example due to an interference in communications between the base station and the mobile station in the middle of multicast data reception.

Alternatively to transmitting (211) all the required keys to the mobile station after all the data was received by the mobile stations, some or all of the keys are provided before the multicast transmission and/or along with the multicast transmission. In some embodiments of the invention, some of the keys are provided in a multicast transmission.

The implementation of the present invention allows using relatively simple encryption methods, since in order to reconstruct a file the receiver needs to break the code for a plurality of different keys. In addition, even if a subscriber succeeds in breaking the code and determining the keys for the data it received, most other users cannot reconstruct the file using these keys as they need other keys. In some embodiments of the invention, the encryption method used is sufficiently complex to prevent breaking of the code by small processors, such as hosted by mobile stations 20, but which may be breakable by stronger processors not usually hosted by mobile units. In some embodiments of the invention, the encryption is performed using a single key for both encryption and decryption. Encryption schemes using a single key for encryption and decryption require less processing resources for decryption, than public-private schemes, so that the battery of the mobile units is not drained out too fast.

Optionally, the encryption is performed in accordance with a polynomial encryption method. Alternatively or additionally, the encryption is performed using a low density parity code (LDPC) such as the Tornado code. Alternatively, the encryption is performed using a public/private key scheme. In some embodiments of the invention, when it is desired to minimize the processing power spent on decryption, a low-complexity encryption scheme is used. For example, a streaming encryption scheme based on generator polynomials may be used.

It is noted that when the channel between base stations 50 and mobile stations 20 has a high loss rate, for example, due to high noise levels and/or late tuning of mobile stations 20 onto the channel, the chances of several mobile stations 20 requiring exactly the same keys is

very small. Optionally, the number of keys used is set such that on the average no more than 5-10 users require the same keys. Alternatively or additionally, the number of keys used is selected such that, on the average, in each cell no more than 5-10% of the receivers require the same keys. Further alternatively or additionally, the number of keys used is selected, such that no more than 0.1-1% of the receivers in the network, on the average, require the same set of keys. Further alternatively or additionally, the number of keys used is adjusted according to the importance of the encrypted data.

In the above description, the same encryption methods are used for all the base stations at all times, but with different keys. Alternatively, the encryption methods are varied from time to time in order to make the breaking of the code more difficult. In some embodiments of the invention, each mobile station 20 optionally has software that can decrypt a plurality of different codes. Along with each key received from key server 36, the receiver is optionally provided with identification of a decryption method to be used with the key.

Alternatively to encrypting segments of the same size as the FEC segments, the encryption may be performed on smaller segments. In some embodiments of the invention, the encryption segments do not range over the border between two FEC segments, so that an error in a transmitted encryption segment affects only a single FEC segment.

In an exemplary embodiment of the invention, the DES encryption algorithm is used. The DES encryption algorithm operates on encryption segments of 8 bytes. Optionally, the FEC segments are larger than the encryption segments, for example including 30 bytes in each segment. In some embodiments of the invention, each FEC segment is broken into four portions: three encrypted segments of 8 bytes each, and a non-encrypted segment of 6 bytes.

In some embodiments of the invention, the non-encrypted bytes are located in the same positions of the FEC segments, such that the receivers can determine 20% of the data without decryption. Optionally, these embodiments are used when 20% of the data file cannot be used without the rest of the data. Alternatively or additionally, at least some of the 20% of the data is used to transfer previews, ads and/or other data which is to be supplied to the users for free. Alternatively, the non-encrypted bytes are positioned at different positions in the FEC segments for different FEC segments. Using a substantially even distribution, each position carries 80% encrypted data and 20% unencrypted data. Thus, for each position, a receiver without encryption keys has at most 20% of the data, if no data is lost. This alternative is optionally used when it is not possible to reconstruct the file only with the unencrypted data. It is noted that although the above discussion uses specific numbers for the unencrypted portion,

the principals of the invention may be used also for other ratios between encrypted and non-encrypted data in the FEC segments.

Although the above description relates to using FEC segments, the present invention may be used with other redundancy methods, such as duplication and/or repeated transmission on different channels and/or in different locations.

The above description relates to base stations that serve as multicast transmission points. It is noted that the present invention may be used for other types of multicast transmission points, such as wireless local area network (WLAN) access points. It is noted that the present invention may be used also in networks that have a plurality of different types of multicast transmission points. Furthermore, the present invention may be used with one or more transmission points that transmit signals on a plurality of different channels (e.g., frequency or code channels), each of the channels defining a separate respective cell.

It will be appreciated that the above described methods may be varied in many ways, including, changing the order of steps, and the exact implementation used. The methods of the present invention may be performed in various protocol layers and may be performed for a single transmission system in a plurality of communication protocol layers. It should also be appreciated that the above described methods and apparatus are to be interpreted as including apparatus for carrying out the methods and methods of using the apparatus.

The present invention has been described using non-limiting detailed descriptions of embodiments thereof that are provided by way of example and are not intended to limit the scope of the invention. For example, different keys may be used only for different base stations without changing the keys for different segments of the same block from a same base station. Thus, the bandwidth required for key dissemination is small while risking a local illegal dissemination of keys. It should be understood that features and/or steps described with respect to one embodiment may be used with other embodiments and that not all embodiments of the invention have all of the features and/or steps shown in a particular figure or described with respect to one of the embodiments. Variations of embodiments described will occur to persons of the art.

It is noted that some of the above described embodiments may describe the best mode contemplated by the inventors and therefore may include structure, acts or details of structures and acts that may not be essential to the invention and which are described as examples. Structure and acts described herein are replaceable by equivalents which perform the same function, even if the structure or acts are different, as known in the art. Therefore, the scope of

the invention is limited only by the elements and limitations as used in the claims. When used in the following claims, the terms "comprise", "include", "have" and their conjugates mean "including but not limited to".

CLAIMS

1. A method of multicasting data, comprising:

providing a data block for multicasting;

generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block;

encrypting at least a portion of the generated segments, so as to generate encrypted data units encrypted with a plurality of different keys or encryption methods; and

transmitting the encrypted data units over one or more multicast channels.

2. A method according to claim 1, wherein generating the plurality of segments comprises generating forward error correction (FEC) segments, such that any group of a predetermined number of non-identical segments can be used to reconstruct the data block.

3. A method according to claim 1, wherein generating the plurality of segments comprises generating segments that include a portion of the data block.

4. A method according to claim 1, wherein the plurality of segments include at least one set of duplicate segments.

5. A method according to claim 1, wherein encrypting at least a portion of the segments comprises encrypting such that each data unit represents data from a single segment.

6. A method according to claim 1, wherein encrypting at least a portion of the segments comprises encrypting each segment into a single encrypted data unit.

7. A method according to claim 1, wherein encrypting at least a portion of the segments comprises encrypting data of each segment into a plurality of encrypted data units.

8. A method according to claim 7, wherein encrypting data of each segment into a plurality of encrypted data units comprises leaving a portion of each segment not encrypted.

9. A method according to claim 8, wherein the non-encrypted portions of the segments are used for transferring preview information.

10. A method according to claim 8, wherein the non-encrypted portions are located in different positions in different segments.

11. A method according to claim 8, wherein the non-encrypted portions are located in same positions of substantially all the segments.

12. A method according to claim 1, wherein encrypting at least a portion of at least some of the segments comprises encrypting using a symmetric coding scheme.

13. A method according to claim 1, wherein encrypting using a plurality of different keys or methods comprises encrypting using different keys and substantially same methods.

14. A method according to any of claims 1-12, wherein encrypting using a plurality of different keys or methods comprises encrypting using different methods.

15. A method according to any of claims 1-12, wherein transmitting the encrypted data units comprises transmitting through a plurality of transmission points each of which transmits to different areas.

16. A method according to claim 15, wherein transmitting the encrypted data units comprises transmitting through a plurality of base stations.

17. A method according to claim 15, wherein each transmission point transmits sufficient data required for reconstruction of the data block.

18. A method according to claim 15, wherein at least some of the transmission points transmit data units representing identical segments encrypted using different keys or methods.

19. A method according to claim 18, wherein the transmission points of at least one group of two or more transmission points transmit data units representing identical segments encrypted using same keys and methods.

20. A method according to claim 19, wherein the transmission points included in a group that transmit data units representing identical segments encrypted using same keys and methods vary dynamically over time.

21. A method according to claim 20, wherein the transmission points included in a group that transmit data units representing identical segments encrypted using same keys or methods vary during transmission of data units representing a single data block.

22. A method according to claim 15, wherein at least one of the transmission points transmits data units encrypted using a plurality of different keys or methods.

23. A method according to claims 15, wherein the encrypted data units are transmitted along with an identification of the respective key required to decrypt the data unit.

24. A method according to claim 23, wherein the identification of the key includes a portion which depends on the transmission point through which the data unit is transmitted.

25. A method according to claim 1, wherein the encrypted data units are transmitted along with an identification of the respective key required to decrypt the data unit.

26. A method according to claim 25, wherein the identification of the key is included in a field including redundancy, such that only some of the possible values of the field are valid identifications of keys.

27. A method according to claim 1, wherein encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels, less than a predetermined percentage of receivers of the data block will require, on the average, the same set of keys for decryption.

28. A method according to claim 27, wherein encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels, less than ten percent of the receivers of the data block will require on the average the same set of keys for decryption.

29. A method according to claim 28, wherein encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels, less than one percent of the receivers of the data block will require on the average the same set of keys for decryption.

30. A method according to claim 1, comprising receiving requests for keys required for decryption and keeping track of receivers that request a suspiciously large number of keys and/or request keys corresponding to non-existent identifications.

31. A method according to claim 1, wherein substantially all the encryption is performed at the same unit.

32. A method according to any of claims 1-12, wherein the encryption of different segments is performed by different units.

33. A method of receiving multicast data over a transmission network, by a mobile station, comprising:

receiving one or more data units of a data block, from each of a plurality of multicast transmission points, the data units of each transmission point being encrypted using different respective one or more keys;

decrypting the data units; and

reconstructing the data block from the decrypted data units, which were received from the plurality of multicast transmission points.

34. A method according to claim 33, comprising determining from the received data units identification of the keys required in order to decrypt the data units and requesting the required keys from a key server.

35. A method according to claim 34, wherein the identifications of the keys depend, at least partially, on the multicast transmission point through which the data units are received, such that data units transmitted through different transmission points include different key identifications.

36. A method according to claim 33, wherein the multicast transmission points comprise base stations.

37. A method according to claim 33, wherein the multicast transmission points comprise one or more wireless LAN access points.

38. A method of multicasting data, comprising:

providing a data block for multicasting;

generating a plurality of different sets of encrypted segments requiring different sets of decryption keys, to represent the data block; and

transmitting each of the different sets of encrypted segments from a different multicast transmission point.

39. A method according to claim 38, wherein generating the plurality of different sets of encrypted segments comprises generating a single set of non-encrypted segments and generating the plurality of different sets of encrypted segments by encrypting the non-encrypted segments using a plurality of different encryption keys.

40. A method according to claim 38, wherein generating the plurality of different sets of encrypted segments comprises encrypting each of the plurality of different sets using groups of different keys.

41. A method according to claim 40, wherein the groups of different keys do not include any common keys.

42. A method according to claim 40, wherein the transmission points comprise base stations of a cellular network.

43. A method according to claim 40, wherein generating the plurality of different sets of encrypted segments is performed in a single encryption unit.

44. A method according to claim 40, wherein at least part of the generating of the sets of encrypted segments is performed separately for each set in respective processors associated with the transmission points.

45. A method according to claim 38, wherein each of the encrypted segments includes a key identification field which identifies the key required to decrypt the segment.

46. A method according to claim 38, comprising providing keys required for decrypting a plurality of sets of segments to a single receiver.

47. A method according to claim 38, comprising providing no more than 50% of the keys used for segments related to the data block to any single receiver.

48. A method of multicasting data, comprising:

providing a data block;

generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block;

encrypting a portion of each of the generated segments, so as to generate respective transmission segments including both encrypted and non-encrypted data; and

transmitting the transmission data units over a multicast channel.

49. A method of multicast transmission comprising:

providing a data block;

encrypting the data block utilizing at least one given key;

multicast transmitting the encrypted data block;

requesting the at least one key by a receiver that receives the encrypted data block; and

unicast transmitting the at least one key to the receiver.

50. A method according to claim 49, wherein encrypting the data block comprises generating a plurality of segments that represent the data block, such that a receiver needs to

receive fewer than all the generated segments in order to reconstruct the data block and encrypting at least some of the segments.

51. A method according to claim 50, wherein encrypting at least some of the segments comprises encrypting one or more of the segments utilizing a first key and using at least one other key for at least one other segment.

52. A method according to claim 49, wherein requesting the at least one key comprises requesting based on an identification of the key included in the transmission.

53. A method according to claim 52, wherein the identification of the key is included in a field that can receive more values than valid identification values.

54. A method according to claim 49, comprising identifying receivers that request a suspiciously large number of keys or request non-existent keys.

55. A method according to claim 49, wherein requesting the at least one key is performed only after the receiver determined that a sufficient amount of data was received to allow reconstruction of the data block.

ABSTRACT

A method of multicasting data. The method includes providing a data block for multicasting, generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block, encrypting at least a portion of the generated segments, so as to generate encrypted data units encrypted with a plurality of different keys or encryption methods and transmitting the encrypted data units over one or more multicast channels.

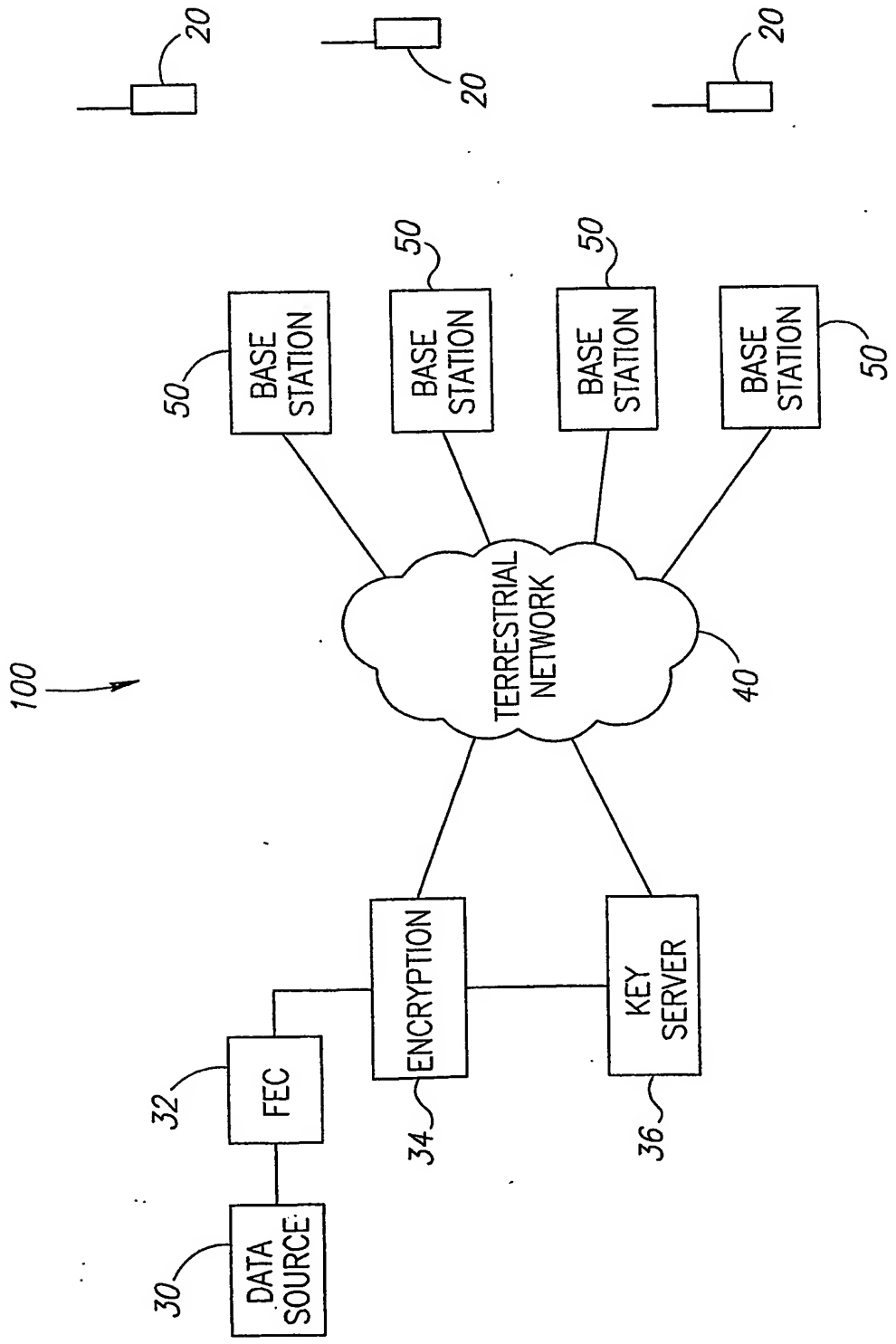
100
20
20
20
50
50
50
50
BASE STATION
BASE STATION
BASE STATION
BASE STATION
TERRESTRIAL NETWORK
40
ENCRYPTION
KEY SERVER
34
36
FEC
32
DATA SOURCE
30

FIG.1

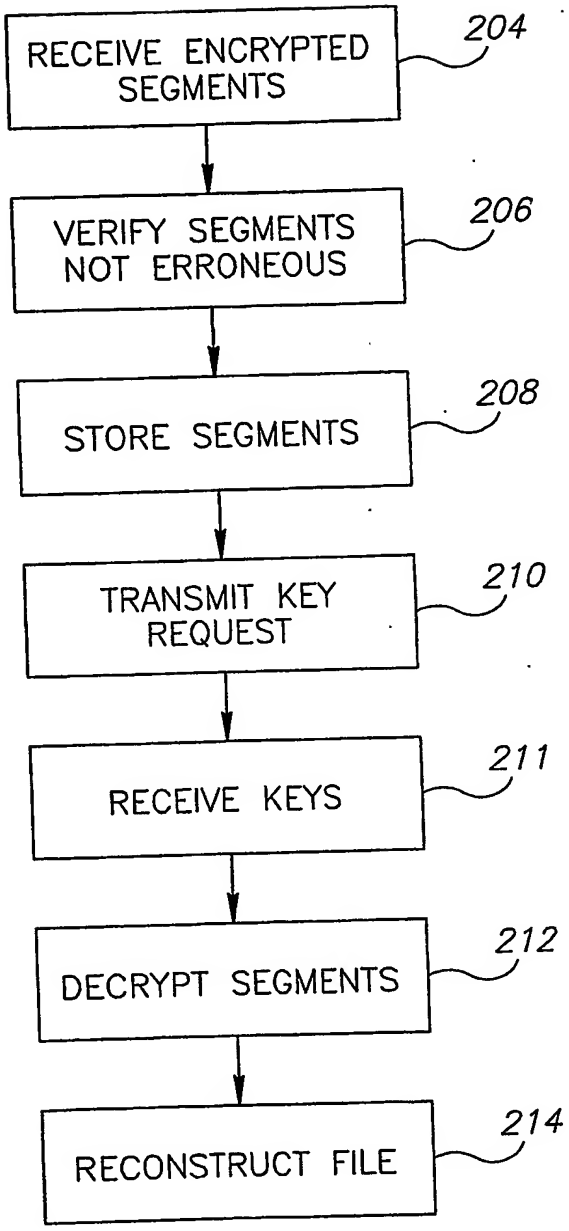
RECEIVE ENCRYPTED SEGMENTS
204
VERIFY SEGMENTS NOT ERRONEOUS
206
STORE SEGMENTS
208
TRANSMIT KEY REQUEST
210
RECEIVE KEYS
211
DECRYPT SEGMENTS
212
RECONSTRUCT FILE
214

FIG.2